WHAT IS CLAIMED IS:

1. A method for intercepting data exchanged by remote terminals (Tij-k), via a communications network, in the form of control packets formatted according to a first real-time data transfer control protocol and associated with data previously exchanged by the said terminals, characterised in that it comprises a step in which i) in the case of transfer of data packets between at least two remote terminals (Tij-k), at least certain of the said packets are intercepted during the said transfer so as to determine those which are formatted according to the said first protocol, then ii) at least part of each packet thus formatted, referred to as a "control packet", is duplicated, and iii) data representing the said duplicated part are communicated to a control application (1) located in the said network, so that it deduces therefrom information on the said transfer.

2. A method according to Claim 1, characterised in that all the control packets transferred are intercepted.

3. A method according to Claim 1, characterised in that the control packets are sampled so as to intercept only one sample from amongst n, n being a chosen integer value.

4. A method according to Claim 1, characterised in that determination of the formatting according to the first protocol concerns the determination, amongst the packets, of those in which at least a network address field for the terminal which sent the packet, a network address field for the destination terminal of the packet, a destination port field and/or a source port field, and a protocol number field have chosen values.

5. A method according to Claim 4, characterised in that the said chosen values are communicated by an application and/or an item of equipment in the network.

6. A method according to Claim 1, characterised in that, between interception and duplication, a comparison is performed between a chosen threshold value and the value of a service information field contained in the intercepted control packet, in order to duplicate only the part at least of the control packet in which the service information field has a value substantially greater than the said threshold value.

7. A method according to Claim 6, characterised in that the whole of each intercepted control packet, formatted according to the first protocol and in which the service information field has a value substantially greater than the said threshold value, is duplicated, and in that the whole of the said duplicated control packet is communicated.

8. A method according to Claim 6, characterised in that certain chosen fields contained in each intercepted control packet, formatted according to the first protocol and in which the service information field has a value substantially greater than the said threshold value, are duplicated, and in that the said duplicated fields are communicated.

9. A method according to Claim 8, characterised in that one of the duplicated and communicated fields is the said service information field.

10. A method according to Claim 8, characterised in that the said service information field is also duplicated, and in that information data representing the said duplicated service information field are communicated with the other duplicated fields.

11. A method according to Claim 1, characterised in that certain chosen fields contained in each intercepted control packet, formatted according to the first protocol, including at least a service information field, are duplicated.

12. A method according to Claim 11, characterised in that information data representing the said duplicated service information field are communicated with the other duplicated fields.

13. A method according to Claim 6, characterised in that the service information field comprises data representing the quality of service.

14. A method according to the combination of Claim 4 with Claim 8, characterised in that the said detected network address field for the terminal which sent the packet, the said detected network address field for the destination terminal of the packet, the said detected destination port field and the said detected protocol number field are duplicated.

15. A method according to Claim 1, characterised in that the whole of each intercepted control packet, formatted according to the first protocol, is duplicated.

16. device for intercepting data exchanged by remote terminals (Tij-k), via a communications network, in the form of packets formatted according to a first real-time data transfer control protocol and associated with data previously exchanged by the said terminals, characterised in that it comprises interception means (2) suitable, in the case of transfer of data packets between at least two remote terminals (Tij-k), for intercepting at least certain of the said packets during the said transfer, and for determining amongst the intercepted packets those which are formatted according to the said first protocol, referred to as "control packets", and management means (3) suitable for duplicating at least part of each intercepted control packet, and for generating data representing the said duplicated part, intended to be communicated to control means (1) located in a control application (S) of the said network.

17. A device according to Claim 16, characterised in that the said interception means (2) are organised for intercepting all the control packets transferred with a view to determining their format.

18. A device according to Claim 17, characterised in that the said interception means (2) are organised for sampling the control packets in the process of being transferred, and for intercepting only one sample from amongst n, n being a chosen integer value, with a view to determining its format.

19. A device according to Claim 16, characterised in that the said interception means (2) are organised for i) detecting from amongst the packets those in which at least a network address field for the terminal which sent the packet, a network address field for the destination terminal of the packet, a destination port field and/or a source port field, and a protocol number field have chosen values, and ii) retaining the packets having the said chosen values, these packets then being referred to as intercepted control packets.

20. A device according to Claim 19, characterised in that the said interception means (2) are organised for receiving the said chosen values from an application and/or from an item of equipment in the network.

21. A device according to Claim 16, characterised in that the said interception means (2) are organised for detecting a service information field contained in each intercepted control packet, and for performing, between interception and duplication, a comparison between a stored chosen threshold value and the value of the detected service information field, so that the management means (3) duplicate only the part at least of the control packet in which the service information field has a value substantially greater than the said threshold value.

22. A device according to Claim 21, characterised in that the said interception means (2) are organised for communicating to the said management means (3) the whole of each intercepted control packet in which the service information field has a value substantially greater than the said threshold value, and in that the said management means (3) are organised for duplicating the whole of each intercepted control packet received, and communicating to the said control means the whole of the said duplicated control packet.

23. A device according to Claim 21, characterised in that the said interception means (2) are organised for communicating to the said management means (3) certain chosen fields contained in each intercepted control packet in which the service information field has a value substantially greater than the said threshold value, and in that the said management means (3) are organised for duplicating the said chosen fields of each intercepted control packet received and communicating the said duplicated fields to the said control means.

24. A device according to Claim 23, characterised in that one of the duplicated and communicated fields is the said service information field.

25. A device according to Claim 23, characterised in that the said interception means (2) are organised for communicating the said service information field to the said management means (3), and in that the said management means (3) are organised for duplicating the said service information field and communicating, with the other duplicated fields, information data representing the said duplicated service information field.

26. A device according to Claim 16, characterised in that the said management means (3) are organised for duplicating certain chosen fields contained in each intercepted control packet, formatted according to the

first protocol, including at least a service information field.

27. A device according to Claim 23, characterised in that the said management means (3) are organised for communicating information data, representing the said duplicated service information field, in addition to the other duplicated fields.

28. A device according to Claim 21, characterised in that the service information field comprises data representing the quality of service.

29. A device according to the combination of Claim 19 with Claim 21, characterised in that the said management means (3) are organised for duplicating the said network address field for the terminal which sent the intercepted packet, the said network address field for the destination terminal of the intercepted control packet, the said destination port field and the said protocol number field, and for communicating the said duplicated fields to the control means (1).

30. A device according to Claim 16, characterised in that the said management means (3) are organised for duplicating the whole of each intercepted control packet, formatted according to the first protocol, and for communicating to the said control means (1) the whole of the said duplicated control packet.

31. A device according to Claim 16, characterised in that the said interception means (2) are located in at least one of the items of network equipment through which the streams intended for the said terminals flow.

32. A device according to Claim 16, characterised in that the said management means (3) are located in at least one of the items of equipment (RC-k; RPj-k) in the network to which the said terminals (Tij-k) are connected.

33. A device according to Claim 31, characterised in that the network equipment is chosen from a group

comprising routers, NAT boxes, firewalls and traffic shapers.

34. Use of the method and device according to one of the preceding claims in networks chosen from amongst public and private networks.

35. Use according to Claim 34, characterised in that the network is the Internet.

36. Use according to Claim 34, characterised in that the first protocol is called RTCP, and is associated with a real-time data transfer protocol called RTP.

37. Use according to Claim 34, characterised in that the duplicated data are communicated according to a protocol chosen from a group comprising the COPS and SNMP protocols, and the encapsulation protocols.